PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets 7 :		(11) Numér de publication internationale:
G07F 19/00, 17/16, G06F 1/00	A1	WO 00/63859
		(43) Date de publication internationale: 26 octobre 2000 (26.10.00)

(21) Numéro de la demande internationale: PCT/FR00/01023

(22) Date de dépôt international: 19 avril 2000 (19.04.00)

(30) Données relatives à la priorité:
99/04963 20 avril 1999 (20.04.99) FR

(71) Déposant *(pour tous les Etats désignés sauf US)*: FRANCE TELECOM [FR/FR]; 6, place d'Alleray, F–75015 Paris (FR).

(72) Inventeurs; et
(75) Inventeurs/Déposants *(US seulement)*: PAILLES, Jean–Claude [FR/FR]; 4, rue des Loisirs, F–14610 Epron (FR). MICHON, Philippe [FR/FR]; 96, avenue H. Cheron, F–14000 Caen (FR). PETIT, Stéphane [FR/FR]; App. 146, Bât Les Iris, Résidence du Nouveau Bassin, 32, rue de Ver, F–14470 Courseules/Mer (FR).

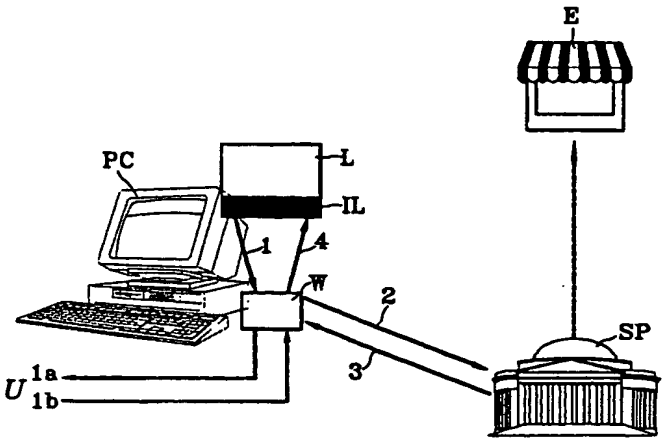
(74) Mandataire: POULIN, Gérard; Société de Protection des Inventions, 3, rue du Docteur Lancereaux, F–75008 Paris (FR).

(81) Etats désignés: AU, CA, CN, IN, JP, RU, US, brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Publiée
Avec rapport de recherche internationale.

(54) Title: PAYMENT SYSTEM FOR SOFTWARE USE

(54) Titre: SYSTEME DE PAIMENT POUR L'UTILISATION DE LOGICIELS



(57) Abstract

The invention concerns a payment system for use of software, comprising an software interface (IL), a payment module (W), a payment server (SP) connected to the software editor (E). The offer for use consists in a message (2), a payment request (2), a payment (3), (4). The invention is useful for controlling the use of software.

(57) Abrégé

Système de paiement pour l'utilisation d'un logiciel. Le système comprend une interface logicielle (IL), un module de paiement (W), un serveur de paiement (SP) en liaison avec l'éditeur du logiciel (E). L'offre d'utilisation fait l'objet d'un message (2), d'une demande de paiement (2), d'un acquittement (3, 4). Application au contrôle de l'utilisation des logiciels.

UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AL	Albanie	**ES**	Espagne	**LS**	Lesotho	**SI**	Slovénie
AM	Arménie	**FI**	Finlande	**LT**	Lituanie	**SK**	Slovaquie
AT	Autriche	**FR**	France	**LU**	Luxembourg	**SN**	Sénégal
AU	Australie	**GA**	Gabon	**LV**	Lettonie	**SZ**	Swaziland
AZ	Azerbaïdjan	**GB**	Royaume-Uni	**MC**	Monaco	**TD**	Tchad
BA	Bosnie-Herzégovine	**GE**	Géorgie	**MD**	République de Moldova	**TG**	Togo
BB	Barbade	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tadjikistan
BE	Belgique	**GN**	Guinée	**MK**	Ex-République yougoslave de Macédoine	**TM**	Turkménistan
BF	Burkina Faso	**GR**	Grèce			**TR**	Turquie
BG	Bulgarie	**HU**	Hongrie	**ML**	Mali	**TT**	Trinité-et-Tobago
BJ	Bénin	**IE**	Irlande	**MN**	Mongolie	**UA**	Ukraine
BR	Brésil	**IL**	Israël	**MR**	Mauritanie	**UG**	Ouganda
BY	Bélarus	**IS**	Islande	**MW**	Malawi	**US**	Etats-Unis d'Amérique
CA	Canada	**IT**	Italie	**MX**	Mexique	**UZ**	Ouzbékistan
CF	République centrafricaine	**JP**	Japon	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Pays-Bas	**YU**	Yougoslavie
CH	Suisse	**KG**	Kirghizistan	**NO**	Norvège	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	République populaire démocratique de Corée	**NZ**	Nouvelle-Zélande		
CM	Cameroun			**PL**	Pologne		
CN	Chine	**KR**	République de Corée	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Roumanie		
CZ	République tchèque	**LC**	Sainte-Lucie	**RU**	Fédération de Russie		
DE	Allemagne	**LI**	Liechtenstein	**SD**	Soudan		
DK	Danemark	**LK**	Sri Lanka	**SE**	Suède		
EE	Estonie	**LR**	Libéria	**SG**	Singapour		

SYSTEME DE PAIEMENT POUR L'UTILISATION DE LOGICIELS
DESCRIPTION

Domaine technique

La présente invention a pour objet un système de paiement pour l'utilisation de logiciels. Ces logiciels peuvent être de nature quelconque et par exemple être des logiciels enregistrés sur un support comme les CD-ROM (Compact Disc-Read Only Memory) ou les DVD-ROM (Digital Versatile Disc-Read Only Memory) ou les logiciels téléchargés.

Ils peuvent concerner aussi bien des calculs scientifiques que des jeux, des techniques assistées par ordinateur, du traitement de texte, etc..

Etat de la technique antérieure

Le mode actuel de diffusion des logiciels est principalement le CD-ROM, et sera très bientôt le DVD-ROM. Pour les éditeurs de logiciel se pose de façon de plus en plus aiguë le problème de la copie frauduleuse de ces logiciels. Si, pendant un temps, le format du CD-ROM a empêché la recopie sur un support vierge, actuellement, les disques inscriptibles et les graveurs de CD sont devenus accessibles au niveau du grand public. Le même phénomène ne tardera sans doute pas à advenir dans le cas de la technologie DVD.

Un autre mode possible de diffusion des logiciels, quoique moins usité pour des raisons de performances, est le téléchargement. Il n'est pas approprié aux jeux ayant besoin de très nombreuses images, ou scènes en trois dimensions. En revanche, il

peut se justifier dans d'autres cas. De nombreux logiciels (compilateurs, éditeurs...) entrent dans cette catégorie. Ces logiciels sont en général gratuits, car, du fait de leur volume faible qui les rend téléchargeables, ils seraient très faciles à copier d'un ordinateur à un autre.

Par ailleurs, il est clair que le prix d'achat élevé d'un logiciel est souvent dissuasif pour les utilisateurs. Le coût du support CD-ROM et de sa gravure intervient pour très peu dans ce prix. Le prix d'achat élevé des CD/DVD-ROM actuels correspond avant tout à la rémunération de l'éditeur et des distributeurs des jeux.

Ces observations donnent à penser qu'il existe un besoin pour le paiement à l'acte, ou à la durée ou à la séance de logiciels sur support CD/DVD-ROM, ou des logiciels téléchargés. Ainsi, les éditeurs se rémunèreront sur une base de clients beaucoup plus importante, en fonction de l'utilisation que le client fait de ce logiciel. Globalement, un tel procédé devrait plutôt développer le chiffre d'affaires de la profession. De plus, la copie de support ne présentera plus d'intérêt, puisque de toute façon, il sera nécessaire de payer pour l'utilisation de ce logiciel.

Or, il n'y a pas, à l'heure actuelle de moyens fiables et sûrs pour assurer un paiement pour l'utilisation de logiciels. La présente invention a justement pour but de remédier à cette carence.

Exposé de l'invention

Un système de paiement pour l'utilisation de logiciel doit pouvoir remplir au moins trois fonctions :

- contrôler l'utilisation du logiciel, chaque fois que le logiciel est lancé, ou bien périodiquement, ou bien lorsqu'un événement particulier se produit dans le logiciel (par exemple un changement de "monde" dans un jeu, un passage au deuxième acte d'une pièce de théâtre ou de film...) ; alors, le logiciel doit demander qu'un paiement soit effectué ;
- enregistrer les utilisations, pour faire payer l'utilisateur : si l'utilisateur accepte la demande de paiement, il faut enregistrer cette demande d'une façon sécurisée, pour pouvoir le faire payer ultérieurement ; la sécurisation doit interdire à l'utilisateur d'effacer ses dettes, et le paiement différé doit permettre d'agréger des petits montants, pour pouvoir présenter à l'utilisateur une note globale, périodiquement (une fois par mois, par exemple), pour des raisons pratiques mais aussi du fait des coûts de recouvrement de ces petits montants ;
- reverser périodiquement à l'éditeur du logiciel le montant dû.

Ces fonctions doivent être remplies compte tenu de certaines contraintes :

- les CD-ROM peuvent être étrangers : un système de paiement de logiciel doit donc comporter une dimension trans-frontière, donc des mécanismes

susceptibles d'être déployés internationalement, et une reconnaissance internationale dans des comités de standardisation ;

- l'interface entre logiciel et les moyens de paiement doit être standardisée de façon à ce qu'un développeur de logiciel n'ait pas à programmer lui-même la logique de paiement correspondant à l'emploi de ce logiciel ;
- le système qui enregistre les utilisations doit être capable de déclencher des paiements internationaux pour rémunérer les éditeurs de logiciels dans n'importe quel pays du monde ;
- l'agrégation pour les paiements des utilisateurs et les reversements aux éditeurs de logiciels doit être possible : comme indiqué plus haut, ceci correspond à un objectif de simplicité, mais aussi à un souci de réduction des coûts bancaires ; notamment, dans le cas de transactions vers l'étranger, il serait inefficace (voire néfaste), sur le plan des coûts, de faire trop d'opérations de virements de petits montants.

La présente invention répond à toutes ces exigences en tenant compte de toutes ces contraintes. A cette fin, le système de l'invention comprend un module de paiement et des moyens de traitement de messages et de paiement. Par ailleurs, le logiciel dont on veut contrôler l'utilisation comprend une interface logicielle. Les fonctions de ces moyens sont les suivantes :

- l'interface logicielle est apte à constituer un premier message qui est un message d'offre d'utilisation du logiciel, ce premier message contenant, notamment, l'identité de l'éditeur du logiciel, les paramètres de l'offre, la signature numérique par l'éditeur d'au moins une partie de l'offre, ce premier message étant adressé au module de paiement ;
- le module de paiement est apte à recevoir ce premier message, à l'afficher, à recevoir en retour l'acceptation éventuelle de l'utilisateur du logiciel, et, en cas d'acceptation, à constituer un deuxième message de demande de paiement contenant notamment l'identité de l'utilisateur et celle de l'éditeur, ainsi qu'une preuve que l'utilisateur accepte l'offre, ce module étant apte à adresser ce deuxième message aux moyens de traitement ;
- les moyens de traitement de messages et de paiement sont aptes à recevoir le deuxième message, à contrôler la preuve qu'il contient, à enregistrer la demande de paiement avec au moins l'identité de l'utilisateur et l'identité de l'éditeur du logiciel, le montant à payer, et à créditer l'éditeur dudit montant, ces moyens étant aptes en outre à constituer un troisième message, qui est un message d'acquittement, ce troisième message comprenant, notamment, l'identité des moyens de traitement et une signature numérique de l'offre, ce troisième message étant adressé au module de paiement ;

- le module de paiement est en outre apte à retransmettre ce troisième message à l'interface logicielle ;
- l'interface logicielle est en outre apte à vérifier la signature des moyens de traitement par rapport aux paramètres de l'offre contenue dans le premier message et, en cas de concordance, à autoriser l'utilisation du logiciel.

Dans une première variante, les moyens de traitement de messages et de paiement sont constitués par un serveur de paiement distant relié au module de paiement par un réseau de télécommunications, ce serveur recevant et traitant le deuxième message, constituant et émettant le troisième message. Ce serveur de paiement agrège les crédits élémentaires pour, périodiquement, reverser aux éditeurs le montant qui leur est dû.

Dans une seconde variante les moyens de traitement de messages et de paiement comprennent des moyens sécurisés contenant au moins l'identité de l'utilisateur, ces moyens étant de plus aptes à recevoir le deuxième message, à contrôler la preuve qu'il contient, à enregistrer la demande de paiement et à constituer le troisième message d'acquittement, et comprennent en outre un serveur de paiement distant apte à créditer l'éditeur.

Dans cette variante, les moyens sécurisés peuvent comprendre un lecteur de carte à puce avec une carte à puce contenant l'identité de l'utilisateur, la carte étant apte à recevoir le deuxième message, à

contrôler la preuve qu'il contient, à enregistrer la demande de paiement et à constituer le troisième message d'acquittement.

Régulièrement, l'ensemble des demandes enregistrées dans la carte, qui correspondent à des usages de logiciels, sont rapatriées dans le serveur grâce à un réseau de télécommunications.

La carte peut être du type pré-payée (sous forme par exemple de porte monnaie électronique) ou post-payée.

Pour une carte pré-payée comme pour une carte post-payée, la carte est apte à constituer un fichier des demandes acquittées et des montants correspondants, le message d'acquittement n'étant émis avec sa signature qu'une fois la mise à jour de ce fichier effectuée.

La présente invention a également pour objet, un module de paiement pour système de paiement pour l'utilisation de logiciel, caractérisé en ce qu'il comprend :

- des moyens pour traiter un premier message contenant, notamment, l'identité d'un éditeur de logiciel, des paramètres d'une offre d'utilisation, une signature numérique d'au moins une partie de cette offre,
- des moyens pour émettre ce message vers un utilisateur,
- des moyens pour recevoir une acceptation dudit utilisateur du logiciel,

- des moyens pour constituer un deuxième message de demande de paiement contenant notamment l'identité de l'utilisateur et celle de l'éditeur ainsi qu'une preuve que l'utilisateur accepte l'offre,
- des moyens pour recevoir et traiter un troisième message comprenant une signature numérique constituant une preuve de paiement.

La présente invention a encore pour objet des moyens de traitement de messages et de paiement pour système de paiement pour l'utilisation de logiciel, caractérisés en ce qu'ils comprennent :

- des moyens aptes à recevoir d'un module de paiement un message de demande de paiement contenant notamment l'identité d'un utilisateur et celle d'un éditeur ainsi qu'une preuve que l'utilisateur accepte l'offre d'utilisation d'un logiciel qui lui a été faite,
- des moyens aptes à contrôler cette preuve,
- des moyens aptes à enregistrer la demande de paiement avec au moins l'identité de l'utilisateur et l'identité de l'éditeur du logiciel, le montant à payer et des moyens aptes à créditer l'éditeur dudit montant,
- des moyens aptes en outre à constituer un message d'acquittement, ce message comprenant, notamment, l'identité des moyens de traitement, et une signature numérique qui constitue la preuve du paiement,

- des moyens pour adresser ce message à un module de paiement.

Brève description des figures

- la figure 1 illustre un système conforme à l'invention dans sa première variante ;

- la figure 2 illustre un arbre de certification avec une chaîne de certificats ;

- la figure 3 illustre un système conforme à l'invention dans sa seconde variante.

Description détaillée de modes particuliers de réalisation

On voit, sur la figure 1, un ordinateur personnel PC supposé contenir un logiciel L, dont on veut contrôler l'utilisation. Ce logiciel est associé à une interface logicielle IL, appelée par la suite "MARCHAND", qui communique avec le système de paiement proprement dit. On trouve également un module de paiement W, appelé par la suite "WALLET". A distance se trouve un serveur de paiement SP, relié au module WALLET par une ligne de transmission (non représentée). L'éditeur du logiciel est référencé E.

Dans la variante illustrée sur la figure 1, lorsque le logiciel L a décidé de demander un nouveau paiement, un message d'offre référencé 1 est émis par l'interface MARCHAND à destination du module WALLET. Ce message d'offre peut contenir :

- l'identité de l'éditeur ;

- la description de l'offre, texte compréhensible par l'utilisateur explicitant ce qu'il va obtenir moyennant paiement (par exemple : "30 minutes supplémentaires d'utilisation" ou bien "scène 3 : durée 25 minutes") ;
- le prix (montant, unité monétaire, etc.)
- l'heure et la date interne du PC ;
- un aléa interne ;
- une signature par l'éditeur du logiciel de cette offre, sous la forme S_E (offre$_h$, prix) où offre$_h$ signifie "condensé des données de l'offre".

Le module WALLET recevant ce message va demander à l'utilisateur U s'il est d'accord pour accepter cette offre. Par exemple, une fenêtre est affichée à l'écran, visualisant la description de l'offre, l'heure et la date, le montant et l'unité monétaire à payer, et ce même prix converti en Francs français. Cet affichage est symbolisé par la flèche 1a sur la figure 1.

Si l'utilisateur U est d'accord, il clique par exemple sur une case " accord " (réponse symbolisée par la flèche 1b sur la figure 1). Le module WALLET émet alors le message 2 "demande de paiement" à destination du serveur SP. Ce message peut contenir :

- un condensé de l'offre$_h$, le prix, la date et l'heure, l'aléa, la signature S_E(offre$_h$, prix) ;
- l'identité de l'utilisateur U, et celle de l'éditeur E ;

- une preuve que le client est d'accord pour acheter cette offre. La nature de la preuve peut dépendre du mode de réalisation : ce peut être un mot de passe envoyé au serveur de paiement SP, ou un code confidentiel donné à une carte à puce, qui elle-même fournit au serveur SP une preuve cryptographique : signature, etc..

Le fait de transmettre un condensé de l'offre ("$offre_h$") et non l'offre complète permet au client de ne pas révéler au serveur SP ce qu'il sélectionne, sans empêcher les contrôles par le serveur SP.

Le serveur de paiement SP recevant cette demande de paiement 2 effectue alors les opérations suivantes :

- contrôle de la preuve donnée par le client,
- conversion en Francs français, si nécessaire,
- contrôle de la consommation de l'utilisateur ; à titre d'exemple, le serveur SP vérifie que le cumul de ce qui a été consommé depuis le début de la période est inférieur au montant d'autorisation attribué à cet utilisateur (cas du post-paiement), ou bien que ce cumul est inférieur à la provision constituée par l'utilisateur à cet usage (cas du pré-paiement),
- enregistrement de la demande de paiement, pour pouvoir réaliser ultérieurement les opérations de paiement ; cet enregistrement comporte au moins :
  - -l'identification de l'utilisateur,
  - -l'identification de l'éditeur du logiciel,
  - -le prix,

-l'heure et date, le condensé $offre_h$ ....,

- constitution du message 3 d'acquittement, qui va prouver au logiciel et à son interface "MARCHAND" que le paiement a bien été réalisé ; ce message d'acquittement, pour établir une preuve vérifiable, contiendra :

-l'identité du serveur SP,

-la signature S_{SP} ($offre_h$, prix, aléa, date-heure) par le serveur de paiement,

Le module WALLET transmet simplement le message reçu à l'interface MARCHAND.

L'interface MARCHAND vérifie la signature S_{SP}($offre_h$, prix, aléa, date-heure) du message d'acquittement, par rapport aux paramètres de l'offre précédemment envoyée. S'il y a concordance, alors l'exécution du logiciel L peut continuer.

Périodiquement, tous les mois par exemple, le serveur SP calcule le cumul des dépenses engagées par chaque utilisateur, et il provoque, dans le cas d'un post-paiement, le paiement effectif des sommes dues au moyen d'une carte pour lequel la connaissance préalable du numéro de carte du client est nécessaire, ou par prélèvement automatique sur le compte du client.

Pour le pré-paiement, ceci se fait par le rechargement volontaire par l'utilisateur de sa provision chez un intermédiaire.

De même, le cumul par l'éditeur permet de calculer le montant dû à chaque éditeur.

Les traits pointillés du dessin de la figure 1 correspondent à ce flux financier du serveur SP vers l'éditeur.

Pour l'établissement des différentes signatures mentionnées ci-dessus, on peut utiliser un système à clé publique avec arbre de certification. Cette solution est en effet l'une des rares qui permettent de concevoir des systèmes simples, sûrs, ouverts et internationalement reconnus.

Les principes de cette technique sont bien connus. La mise en œuvre est schématisée sur la figure 2. Une autorité A définit la "racine" de l'arbre de certification, dans lequel se trouvent les différents acteurs du système :

- les éditeurs de logiciels utilisant ce moyen de paiement,
- les serveurs SP,
- les entités intermédiaires ; dans l'exemple de la figure 2, il pourrait s'agir d'un syndicat d'éditeurs de logiciels d'un pays (SYND), et d'une autorité nationale de régulation des serveurs INTERNET (SINT).

Ainsi, lorsqu'un logiciel de tel éditeur de logiciel est utilisé par un utilisateur correspondant à tel serveur SP, un ou des certificats joints aux messages 1 et 3 permettent de vérifier les signatures.

Pour le message d'offre (message 1) l'éditeur E peut adresser au serveur SP un message contenant le condensé $offre_h$, le prix, la date et l'heure, l'aléa, la

signature $S_E(offre_h, prix)$, le certificat de E par SYND, le certificat de SYND par A.

Le serveur SP, qui connaît la clé publique de A, vérifie le certificat de SYND par A, avec la clé publique de A. Il obtient donc la clé publique de SYND, de façon sûre et vérifie le certificat de E par SYND avec la clé publique de SYND. Il obtient alors la clé publique de E, de façon sûre, et peut finalement contrôler la signature S_E.

La variante qui vient d'être décrite peut être qualifiée de "en ligne" ("on line") car l'utilisateur doit se connecter, par exemple par le réseau INTERNET, au serveur SP à chaque demande de paiement. Cette version n'est acceptable que pour des paiements peu fréquents (par exemple pour pouvoir recevoir un film sur DVD-ROM qui dure 2 heures).

L'invention prévoit une autre variante, qui est mieux appropriée aux paiements répétés. Cette variante est décrite sur la figure 3. Elle suppose l'existence d'un lecteur de carte LC et d'une carte C. Comme la carte constitue un support sûr, elle remplace le serveur SP en ce qui concerne les messages 2 et 3, lesquels circulent alors entre le module W et le lecteur de carte LC. Cette variante peut être qualifiée de "off line" (hors connexion) par opposition à la première. Le paiement de l'éditeur E s'effectue toujours par le serveur de paiement SP, lequel reçoit périodiquement les informations mémorisées dans la carte (ligne PP).

S'agissant de la carte C, on peut distinguer deux cas :

- la carte est une carte pré-payée (du type carte porte-monnaie électronique, par exemple) ; la provision financière diminue à chaque fois qu'un message de demande de paiement est traité ; alors, il n'y a pas de risque d'impayés, car la carte avant de se vider, a du être chargée ; il faut cependant relever les utilisations qui ont été faites, pour pouvoir payer les éditeurs, selon l'utilisation de leurs logiciels ; ceci peut par exemple être fait au moment du rechargement de la carte ;
- la carte est une carte post-payée : le risque existe que les utilisations enregistrées dans la carte ne reviennent jamais à l'intermédiaire, donc que le client ne soit jamais débité, et par voie de conséquence que les éditeurs des logiciels utilisés ne soient pas crédités. La parade à ce problème consiste à limiter les paiements à un certain plafond et/ou à faire payer une caution supérieure à ce plafond, qui dissuade l'utilisateur de faire disparaître sa carte.

Du point de vue des mécanismes précis, cette seconde variante reste très proche de la première, si ce n'est le remplacement du serveur SP par la carte C. Cette carte devra donc contenir un fichier des utilisations qui, comme dans le cas du serveur SP, contiendra les enregistrements des transactions, eux mêmes contenant au minimum les informations suivantes :

- l'identification de l'utilisateur,
- l'identification de l'éditeur du logiciel,
- le prix.

Si l'on accepte de sacrifier un peu de sécurité pour ne pas avoir le surcoût du lecteur de carte, la carte pourra être remplacée par un moyen de mémorisation intégré au PC.

Pour que le fichier des demandes de paiement ne soit pas trop facilement altérable ou effaçable, il faut utiliser des techniques de fragmentation/ dissémination sur la totalité du disque, dont la complexité constituera une barrière, certes moins forte que la sécurité physique des cartes à puce, mais suffisante dans bien des cas.

REVENDICATIONS

1. Système de paiement pour l'utilisation d'un logiciel (L) contenu sur un support, ce logiciel contenant une interface (IL), le système comprenant un module de paiement (W) et des moyens de traitement de messages et de paiement (SP), les fonctions de ces moyens étant les suivantes :

l'interface logicielle (IL) est apte à constituer un premier message (1) qui est un message d'offre d'utilisation du logiciel, ce premier message (1) contenant, notamment, l'identité de l'éditeur du logiciel (E), des paramètres de l'offre, la signature numérique par l'éditeur d'au moins une partie de l'offre, ce premier message étant adressé au module de paiement (W) ;

le module de paiement (W) est apte à recevoir ce premier message (1), à l'afficher (1a), à recevoir en retour l'acceptation éventuelle (1b) de l'utilisateur (U) du logiciel, et en cas d'acceptation, à constituer un deuxième message (2) de demande de paiement contenant notamment l'identité de l'utilisateur (U) et celle de l'éditeur (E) ainsi qu'une preuve que l'utilisateur (U) accepte l'offre, ce module (W) étant apte à adresser ce deuxième message (2) aux moyens de traitement de messages et de paiement (SP) ;

les moyens de traitement de messages et de paiement (SP) sont aptes à recevoir le deuxième message (2), à contrôler la preuve qu'il contient, à enregistrer la demande de paiement avec au moins

l'identité de l'utilisateur (U) et l'identité de l'éditeur du logiciel (E), le montant à payer et à créditer l'éditeur (E) dudit montant, ces moyens étant aptes en outre à constituer un troisième message (3), qui est un message d'acquittement, ce troisième message (3) comprenant, notamment, l'identité des moyens de traitement et une signature numérique qui constitue la preuve du paiement, ce troisième message étant adressé au module de paiement (W) ;

le module de paiement (W) est en outre apte à retransmettre ce troisième message (3) à l'interface logicielle (IL) ;

l'interface logicielle (IL) est en outre apte à vérifier la signature des moyens de traitement par rapport aux paramètres de l'offre contenue dans le premier message et, en cas de concordance, à autoriser l'utilisation du logiciel (L).

2. Système selon la revendication 1, dans lequel la signature numérique par l'éditeur d'au moins une partie de l'offre et la signature numérique constituant la preuve du paiement, sont des signatures à clé publique avec arbre de certification, une autorité (A) définissant une racine de l'arbre de certification dans lequel se trouvent les différents acteurs du système, notamment les éditeurs de logiciels (E) et les serveurs de paiement (SP), un ou des certificats étant joint(s) au premier et au troisième messages (1) (3) pour la vérification des signatures.

3. Système selon la revendication 1, dans lequel les moyens de traitement de messages et de paiement sont constitués par un serveur de paiement distant (SP) relié au module de paiement (W) par un réseau de télécommunications, ce serveur (SP) recevant et traitant le deuxième message (2) et constituant et émettant le troisième message (3), ce serveur de paiement calculant le cumul des dépenses engagées par chaque utilisateur pour tous les éditeurs pour faire payer cet utilisateur, et provoquant le reversement des sommes dues à chaque éditeur par tous les utilisateurs.

4. Système selon la revendication 1, dans lequel les moyens de traitement de messages et de paiement comprennent des moyens sécurisés (LC, C) contenant au moins l'identité de l'utilisateur (U), ces moyens étant aptes à recevoir le deuxième message (2), à contrôler la preuve qu'il contient, à enregistrer la demande de paiement et à constituer le troisième message d'acquittement (3) avec la preuve de paiement, et comprennent en outre un serveur de paiement distant (SP) apte à créditer l'éditeur (E).

5. Système selon la revendication 4, dans lequel les moyens sécurisés comprennent un lecteur de carte (LC) avec une carte (C) contenant l'identité de l'utilisateur, le lecteur de carte et la carte étant aptes à recevoir le deuxième message (2), à contrôler la preuve qu'il contient, à enregistrer la demande de paiement et à constituer le troisième message d'acquittement (3) avec la preuve de paiement.

6. Système selon la revendication 5, dans lequel la carte (C) est du type pré-payée et contient une provision, la carte étant apte à débiter cette provision à chaque demande de paiement du montant de la demande.

7. Système selon la revendication 6, dans lequel la carte pré-payée (C) formant le message d'acquittement est apte à insérer, dans ce message, une preuve que le montant de la demande dû a été débité dans la carte.

8. Système selon la revendication 6, dans lequel la carte pré-payée (C) est apte à constituer un fichier des demandes acquittées et des montants correspondants, le message d'acquittement n'étant émis avec sa signature qu'une fois la mise à jour de ce fichier effectuée.

9. Système selon la revendication 8, dans lequel la carte pré-payée (C) peut être rechargée, le fichier qu'elle contient étant transféré préalablement au serveur de paiement (SP) lors du rechargement pour reversement aux éditeurs.

10. Système selon la revendication 6, dans lequel la carte pré-payée (C) est du type porte-monnaie électronique.

11. Système selon la revendication 5, dans lequel la carte (C) est du type post-payée.

12. Système selon la revendication 11, dans lequel la carte post-payée (C) est apte à constituer un fichier des demandes acquittées et des montants correspondants, le message d'acquittement n'étant émis avec sa signature qu'une fois la mise à jour de ce fichier effectué.

13. Système selon la revendication 12, dans lequel le fichier de la carte est transféré au serveur de paiement (SP) pour reversement aux éditeurs.

14. Module de paiement (W) pour système de paiement pour l'utilisation de logiciel, caractérisé en ce qu'il comprend :

- des moyens pour traiter un premier message (1) contenant, notamment, l'identité d'un éditeur de logiciel (E), des paramètres d'une offre d'utilisation, une signature numérique d'au moins une partie de cette offre,
- des moyens pour émettre ce message (1a) vers un utilisateur (U),
- des moyens pour recevoir une acceptation (1b) dudit utilisateur (U) du logiciel,
- des moyens pour constituer un deuxième message (2) de demande de paiement contenant notamment l'identité de l'utilisateur (U) et celle de

l'éditeur (E) ainsi qu'une preuve que l'utilisateur (U) accepte l'offre,

- des moyens pour recevoir et traiter un troisième message (3) comprenant une signature numérique constituant une preuve de paiement.

15. Moyens de traitement de messages et de paiement (SP) pour système de paiement pour l'utilisation de logiciel, caractérisés en ce qu'ils comprennent :

- des moyens aptes à recevoir d'un module de paiement (W) un message de demande de paiement contenant notamment l'identité d'un utilisateur (U) et celle d'un éditeur (E) ainsi qu'une preuve que l'utilisateur (U) accepte l'offre d'utilisation d'un logiciel qui lui a été faite,
- des moyens aptes à contrôler cette preuve,
- des moyens aptes à enregistrer la demande de paiement avec au moins l'identité de l'utilisateur et l'identité de l'éditeur (E) du logiciel, le montant à payer et des moyens aptes à créditer l'éditeur (E) dudit montant,
- des moyens aptes en outre à constituer un message (3) d'acquittement, ce message (3) comprenant, notamment, l'identité des moyens de traitement, et une signature numérique qui constitue la preuve du paiement,
- des moyens pour adresser ce message (3) à un module de paiement (W).

16. Moyens de traitement de messages et de paiement (SP) pour système de paiement pour l'utilisation de logiciel, caractérisés en ce qu'ils comprennent des moyens sécurisés comprenant un lecteur de carte (LC) avec une carte (C) contenant l'identité d'un utilisateur de logiciel, le lecteur de carte et la carte étant aptes à recevoir un message contenant une preuve que l'utilisateur a accepté une offre et à contrôler cette preuve, à enregistrer une demande de paiement et à constituer un message d'acquittement (3) avec la preuve de paiement.

17. Moyens de traitement de messages et de paiement (SP) selon la revendication 16, dans lesquels la carte (C) est du type pré-payée et contient une provision, la carte étant apte à débiter cette provision à chaque demande de paiement du montant de la demande.

18. Moyens de traitement de messages et de paiement (SP) selon la revendication 17, dans lesquels la carte pré-payée (C) formant le message d'acquittement est apte à insérer, dans ce message, une preuve que le montant de la demande dû a été débité dans la carte.

19. Moyens de traitement de messages et de paiement (SP) selon la revendication 17, dans lesquels la carte pré-payée (C) est apte à constituer un fichier des demandes acquittées et des montants correspondants,

le message d'acquittement n'étant émis qu'une fois la mise à jour de ce fichier effectuée.

20. Moyens de traitement de messages et de paiement (SP) selon la revendication 17, dans lesquels la carte pré-payée (C) peut être rechargée, le fichier qu'elle contient pouvant être transféré lors du rechargement.

21. Moyens de traitement de messages et de paiement (SP) selon la revendication 17, dans lesquels la carte pré-payée (C) est du type porte-monnaie électronique.

22. Moyens de traitement de messages et de paiement (SP) selon la revendication 16, dans lesquels la carte (C) est du type post-payée.

FIG. 1

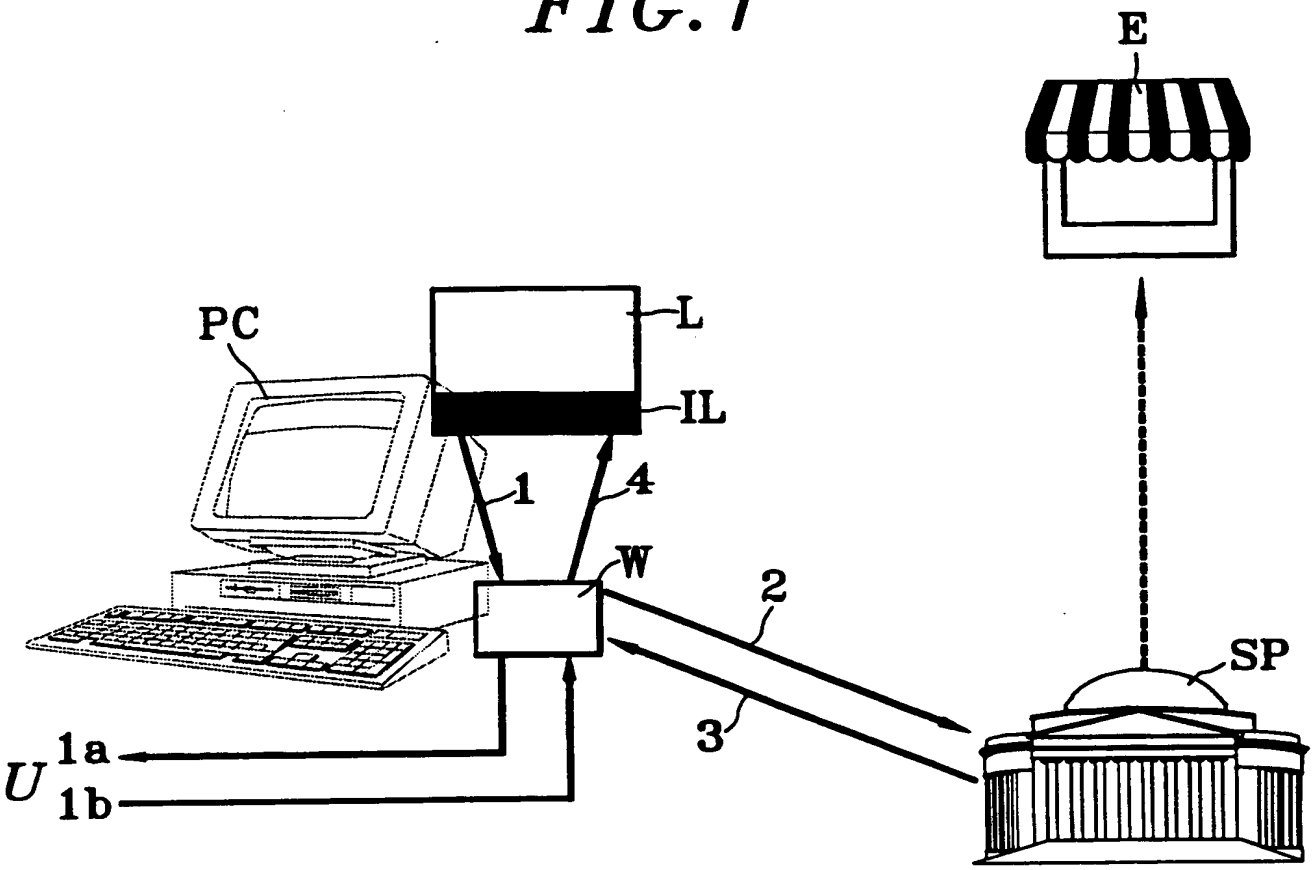


FIG. 2

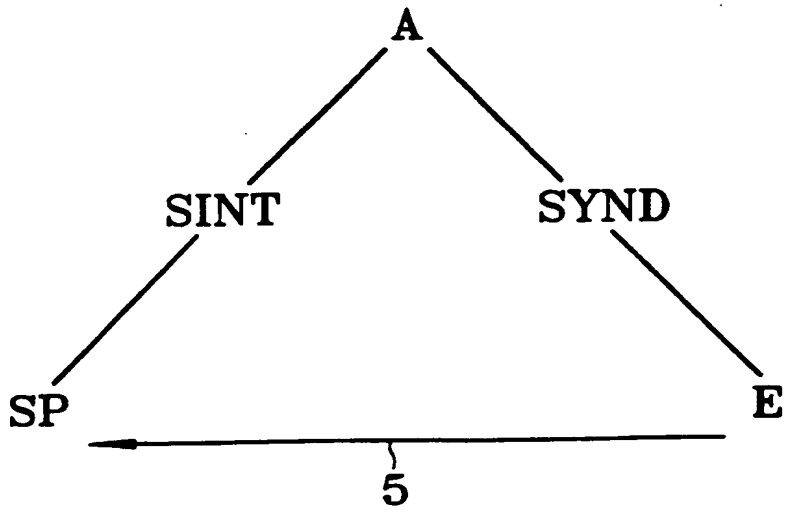
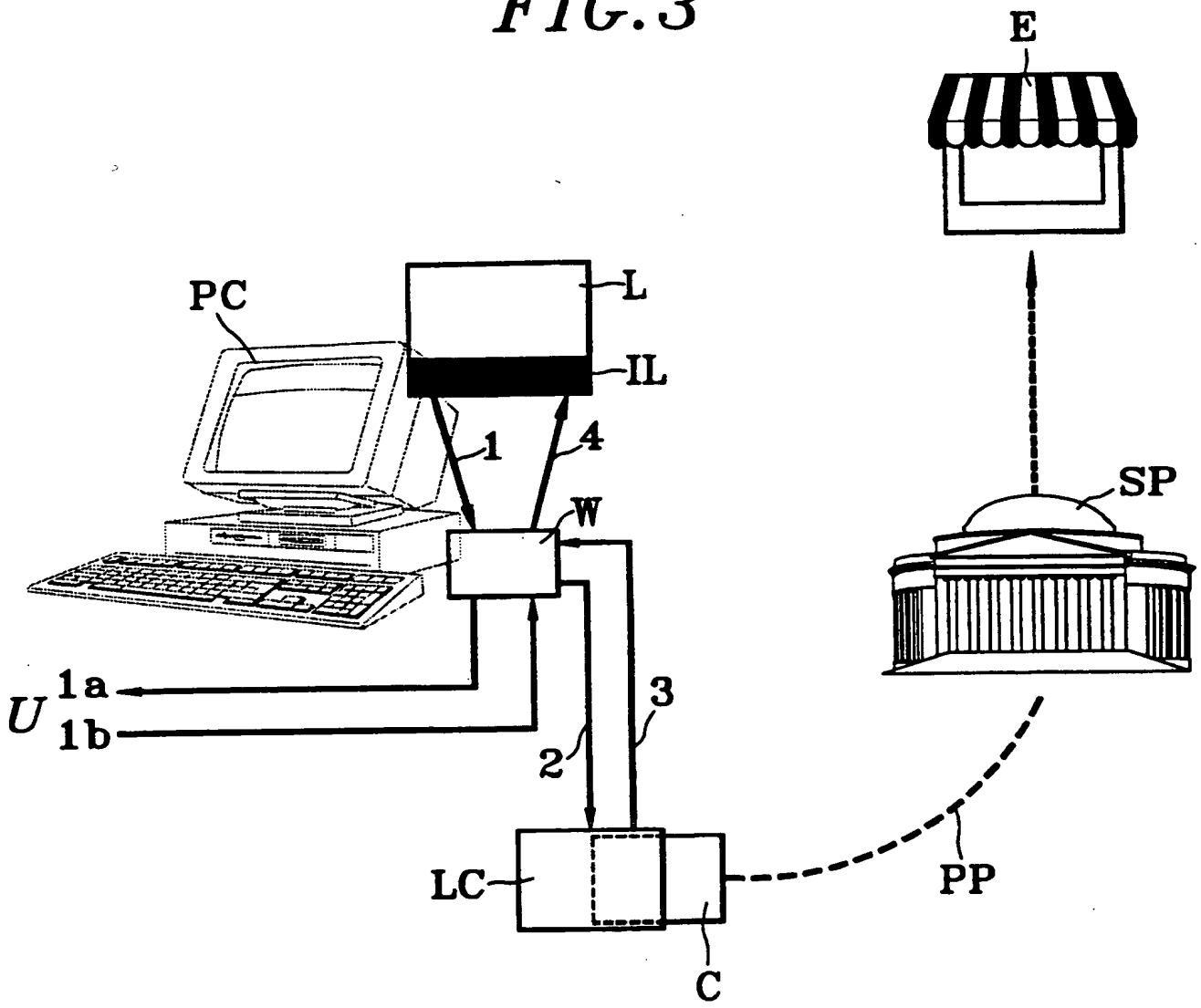


FIG.3



INTERNATIONAL SEARCH REPORT

Inte [redacted] pplication No
PCT/[redacted]00/01023

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F19/00 G07F17/16 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07F H04N G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	WO 95 34857 A (SMITH JAMES P ;SMITH EDWARD A (US)) 21 December 1995 (1995-12-21) page 6, line 1 - line 5 page 6, line 26 -page 7, line 18 page 8, line 6 - line 18 page 8, line 26 -page 9, line 5 page 9, line 29 -page 10, line 5 page 10, line 34 -page 11, line 12 page 11, line 32 -page 12, line 25; claim 1; figures 2,6,7 abstract --- -/--	1,3-5, 14-16 2,6-13, 17-22

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 July 2000	25/07/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Wauters, J

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
X A	EP 0 809 221 A (SUN MICROSYSTEMS INC) 26 November 1997 (1997-11-26) column 1, line 3 - line 7 column 1, line 18 - line 27 column 2, line 49 -column 3, line 6 column 4, line 9 - line 11 column 4, line 39 - line 49 column 5, line 1 - line 49 column 6, line 2 -column 7, line 39 column 8, line 10 - line 18 column 9, line 56 -column 10, line 37; claim 1; figures 1,2,4-6,8 abstract	1,3,4, 14,15 2,5-13, 16-22
Y A	US 5 769 269 A (PETERS STEVEN A) 23 June 1998 (1998-06-23) column 1, line 18 - line 21 column 2, line 49 - line 56 column 8, line 13 - line 24; claim 1; figure 1A abstract	6-13, 17-22 1-5, 14-16
Y	US 4 881 264 A (MERKLE RALPH C) 14 November 1989 (1989-11-14) column 2, line 59 - line 68 column 3, line 19 - line 38; figures 1-3 abstract	2
A	PATENT ABSTRACTS OF JAPAN vol. 1999, no. 02, 26 February 1999 (1999-02-26) & JP 10 312277 A (NAKAMICHI CORP), 24 November 1998 (1998-11-24) abstract	1-22

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int[redacted] Application No
PCT/[redacted] 00/01023

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9534857 A	21-12-1995	AU 2774495 A	05-01-1996
EP 0809221 A	26-11-1997	JP 10222579 A	21-08-1998
US 5769269 A	23-06-1998	AU 2466095 A	29-11-1995
		BR 9507545 A	05-08-1997
		GB 2303238 A,B	12-02-1997
		WO 9530212 A	09-11-1995
US 4881264 A	14-11-1989	NONE	
JP 10312277 A	24-11-1998	NONE	

RAPPORT DE RECHERCHE INTERNATIONALE

Der [redacted]rnationale No
PCT/[redacted]00/01023

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G07F19/00 G07F17/16 G06F1/00

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 G07F H04N G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X Y	WO 95 34857 A (SMITH JAMES P ;SMITH EDWARD A (US)) 21 décembre 1995 (1995-12-21) page 6, ligne 1 - ligne 5 page 6, ligne 26 -page 7, ligne 18 page 8, ligne 6 - ligne 18 page 8, ligne 26 -page 9, ligne 5 page 9, ligne 29 -page 10, ligne 5 page 10, ligne 34 -page 11, ligne 12 page 11, ligne 32 -page 12, ligne 25; revendication 1; figures 2,6,7 abrégé --- -/--	1,3-5, 14-16 2,6-13, 17-22

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
14 juillet 2000	25/07/2000

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Wauters, J

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

[redacted] e internationale No
PCT/FR 00/01023

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	EP 0 809 221 A (SUN MICROSYSTEMS INC) 26 novembre 1997 (1997-11-26)	1,3,4, 14,15
A	colonne 1, ligne 3 - ligne 7 colonne 1, ligne 18 - ligne 27 colonne 2, ligne 49 -colonne 3, ligne 6 colonne 4, ligne 9 - ligne 11 colonne 4, ligne 39 - ligne 49 colonne 5, ligne 1 - ligne 49 colonne 6, ligne 2 -colonne 7, ligne 39 colonne 8, ligne 10 - ligne 18 colonne 9, ligne 56 -colonne 10, ligne 37; revendication 1; figures 1,2,4-6,8 abrégé	2,5-13, 16-22

Y	US 5 769 269 A (PETERS STEVEN A) 23 juin 1998 (1998-06-23)	6-13, 17-22
A	colonne 1, ligne 18 - ligne 21 colonne 2, ligne 49 - ligne 56 colonne 8, ligne 13 - ligne 24; revendication 1; figure 1A abrégé	1-5, 14-16

Y	US 4 881 264 A (MERKLE RALPH C) 14 novembre 1989 (1989-11-14) colonne 2, ligne 59 - ligne 68 colonne 3, ligne 19 - ligne 38; figures 1-3 abrégé	2

A	PATENT ABSTRACTS OF JAPAN vol. 1999, no. 02, 26 février 1999 (1999-02-26) & JP 10 312277 A (NAKAMICHI CORP), 24 novembre 1998 (1998-11-24) abrégé	1-22

1

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale No
PCT/FR00/01023

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
WO 9534857	A	21-12-1995	AU 2774495	A	05-01-1996
EP 0809221	A	26-11-1997	JP 10222579	A	21-08-1998
US 5769269	A	23-06-1998	AU 2466095	A	29-11-1995
			BR 9507545	A	05-08-1997
			GB 2303238	A,B	12-02-1997
			WO 9530212	A	09-11-1995
US 4881264	A	14-11-1989	AUCUN		
JP 10312277	A	24-11-1998	AUCUN		